

**Federal Emergency Management Agency**  
**Information Technology Architecture**  
**Volume 1**



**Version 1.0**  
**November 2, 1998**

This page intentionally left blank

# **Federal Emergency Management Agency**

## **Information Technology Architecture**

### **Volume 1**

**November 2, 1998**

**Version 1.0**

**Prepared by:**

**Federal Emergency Management Agency  
Information Technology Services (ITS) Directorate  
500 C Street, S.W.  
Washington, D.C. 20472**

This page intentionally left blank

## Table of Contents

Table of Contents .....	iii
List of Figures .....	v
List of Tables.....	v
List of Appendices .....	vi
Foreword .....	vii
Executive Summary .....	xi
1. FEMA Enterprise IT Architecture.....	1-1
1.1 Introduction .....	1-1
1.2 Background of Enterprise Architecture.....	1-1
1.3 Directives for Development of the FEMA IT Architecture .....	1-2
1.4 Scope and Definition of the FEMA Enterprise and the Enterprise IT Architecture.....	1-2
1.5 Relationship of the FEMA ITA to Other High-Level Documents .....	1-3
1.6 FEMA’s Mission and Principles .....	1-4
1.6.1 FEMA Mission Statement.....	1-4
1.6.2 FEMA Principles of Operation.....	1-4
1.6.3 Overall FEMA Organization.....	1-6
1.6.4 Missions and Responsibilities of Individual FEMA Organizational Entities.....	1-6
1.6.5 FEMA IT Management Team .....	1-8
1.6.6 FEMA Operational Environment for IT Systems.....	1-10
1.7 FEMA IT Architectural Goals and Objectives .....	1-11
1.8 FEMA IT Architectural Principles .....	1-11
1.9 Snapshot of Current FEMA IT Architecture .....	1-12
1.10 FEMA Target IT Architecture and Requirements for Enhanced Automation .....	1-14
1.11 Mapping of FEMA Target IT Architecture to the NIST Model.....	1-21
1.12 Major IT Architectural Components .....	1-22
1.12.1 Methodology.....	1-22
1.12.2 FEMA Business Processes .....	1-24
1.12.3 FEMA Information Flows and Relationships.....	1-39
1.12.4 FEMA Systems and Applications .....	1-41
1.12.5 FEMA Data Descriptions .....	1-45
1.12.6 FEMA Technology Infrastructure .....	1-50
2. Technical Reference Model (TRM) and Standards Profiles .....	2-1
2.1 Foreword to TRM and Standards Profiles.....	2-1
2.1.1 Introduction to the TRM and Standards Profiles.....	2-1
2.1.2 Background of the TRM and Standards Profiles.....	2-1
2.1.3 Terms and Definitions .....	2-3
2.1.4 Goals and Objectives .....	2-3
2.1.5 CIO Directives for Application of the TRM and Standards Profiles in FEMA IT Systems .....	2-4
2.2 FEMA Technical Reference Model (TRM) .....	2-4
2.2.1 Key Architectural Issues Associated with Standards .....	2-4
2.2.2 Identification and Description of Major FEMA IT Services.....	2-4
2.3 FEMA Standards Profiles.....	2-5
2.3.1 Nature of a Standards Profile .....	2-5
2.3.2 Identification of Major IT Standards in the FEMA High-Level TRM Framework .....	2-5
2.4 FEMA Security Architecture.....	2-5

2.4.1	Preferred Methodology for Development of a Security Architecture .....	2-6
2.4.2	Goals of the FEMA Security Architecture .....	2-6
2.4.3	Security Architecture Development Approach.....	2-6
2.4.4	Security Architecture Methodology .....	2-7
3.	Communications and Networking.....	3-1
3.1	Overview .....	3-1
3.1.1	Network Architecture Components.....	3-1
3.1.2	Network Infrastructure .....	3-1
3.1.3	Network Services .....	3-2
3.1.4	IT Systems.....	3-2
3.1.5	Network Architecture Process.....	3-2
3.2	Existing Network Architecture.....	3-3
3.2.1	Network Infrastructure .....	3-3
3.2.2	Network Services .....	3-7
3.2.3	IT Systems and User Elements.....	3-9
3.3	Requirements and Opportunities.....	3-9
3.3.1	Integration of Backbone Transmission.....	3-10
3.3.2	Voice over Data Networks .....	3-10
3.3.3	Integrated Network and Configuration Management.....	3-10
3.3.4	IP Address Management.....	3-10
3.3.5	Derived ITA Network Requirements .....	3-11
3.4	Target Network Architecture.....	3-12
3.4.1	Overview .....	3-12
3.4.2	Objectives and Criteria.....	3-12
3.4.3	Evaluation of Alternative Backbone Transport Protocols.....	3-14
3.4.4	Target Network Architecture Recommendations.....	3-15
3.5	Recommended Implementation Strategy.....	3-20
3.5.1	Phased Evolutionary Approach .....	3-20
3.5.2	Prototyping .....	3-22
3.5.3	Legacy Support.....	3-23
3.5.4	Event-Driven Milestone Schedule.....	3-23
4.	Maintaining and Implementing the <i>FEMA IT Architecture</i> .....	4-1
4.1	Introduction .....	4-1
4.2	Requirements and Plans for Maintaining and Implementing the IT Architecture.....	4-1
4.2.1	FEMA IT Architecture Change Management .....	4-1
4.2.2	Plans for Implementation of the <i>FEMA IT Architecture</i> .....	4-2
4.2.3	Legacy Systems Integration .....	4-2
4.2.4	CIO and IRB Guidelines for Re-Engineering of Legacy Systems .....	4-3
4.2.5	NEMIS as a FEMA Architectural <i>Cornerstone</i> .....	4-3
4.2.6	Personnel Requirements for Development, Maintenance, and Implementation of the <i>FEMA IT Architecture</i> .....	4-3
4.2.7	IT Industry Coordination and Liaison .....	4-4
4.2.8	Partnership with Other Federal Agencies, State, and Local Governments, and Voluntary Organizations.....	4-4
4.2.9	Understanding of Standards .....	4-5
4.2.10	Strategy and Plans for Hiring, Training, and Professional Development.....	4-5
4.2.11	Seat Management .....	4-5
4.2.12	Employment of Agency Resources vs. Outsourcing .....	4-6
4.2.13	CIO Policies for the <i>IT Architecture</i> .....	4-6

## List of Figures

Figure 1-1	FEMA Organization at the Director, Directorate, Region, and Administration Levels .....	1-6
Figure 1-2	Snapshot of Current <i>FEMA IT Architecture</i> .....	1-12
Figure 1-3	FEMA Enterprise Architectural Concept of Creating, Managing, and Using Documents and Data in an Intelligent Format .....	1-15
Figure 1-4	Integration of IT Systems Environment into the Networking Environment .....	1-16
Figure 1-5	<i>FEMA IT Architecture</i> Target Vision .....	1-17
Figure 1-6	Bandwidth Requirements and Network Characteristics for Various Advanced Information Technologies .....	1-19
Figure 1-7	Mapping of Target <i>FEMA IT Architecture</i> to the NIST Model .....	1-21
Figure 1-8	Structure of FEMA Information Technology Architecture Data Base .....	1-22
Figure 1-9	Framework for Conducting Structured Discussions with FEMA Organizational Elements .....	1-23
Figure 1-10	Federal Response Plan Activities .....	1-33
Figure 1-11	Scope of Structured Discussions on FEMA Information Flow Requirements ...	1-41
Figure 1-12	Target Architecture for Well-Integrated Enterprise Systems and Services .....	1-42
Figure 1-13	Architectural Concept for Integrating Program-Centric Systems .....	1-45
Figure 1-14	Sample NEMIS Logical Data Model .....	1-48
Figure 1-15	Integration of Documents and Data with an Object-Relational Document Model .....	1-49
Figure 1-16	Identification of Reusable Architectural Components for FEMA IT Systems ...	1-51
Figure 2-1	FEMA Target Concept for Implementing Open Systems Standards .....	2-2
Figure 2-2	Generic Systems and Network Representation Approach to Develop the Security Architecture .....	2-8
Figure 3-1	Network Architecture Model .....	3-1
Figure 3-2	National Network Operations Branch (NNOB) .....	3-3
Figure 3-3	FEMA Enterprise Network .....	3-4
Figure 3-4	Switched Network Configuration .....	3-5
Figure 3-5	Switched Network Connectivity .....	3-5
Figure 3-6	Data Network Connectivity .....	3-6
Figure 3-7	Asynchronous Transfer Mode (ATM) .....	3-15
Figure 3-8	FEMA Transmission Media .....	3-16
Figure 3-9	Importance of Protocol Scalability .....	3-17
Figure 3-10	Phased Approach Alternative .....	3-21
Figure 3-11	Hybrid Implementation .....	3-22

## List of Tables

Table 1-1	Missions for FEMA Directorates and Administrations .....	1-7
Table 2-1	Goals and Objectives .....	2-3
Table 3-1	T1 Summary .....	3-7
Table 3-2	Major Network Equipment Types .....	3-7
Table 3-3	Standard Tools Used for Network and Systems Management .....	3-8

## List of Appendices

Appendix A	Acronyms, Terms, and Definitions .....	A-1
Appendix B	References .....	B-1
Appendix C	FEMA and Comprehensive Emergency Management (CEM) References in Public Law, Regulations, and Directives .....	C-1
Appendix D	Catalog of FEMA Program-Centric Systems .....	D-1
Appendix E	FEMA ITA Requirements Traceability Matrix (RTM).....	E-1
Appendix F	High-Level Discussion and Analysis of FEMA Information Flow Requirements.....	F-1
Appendix G	FEMA Enterprise Documents and Data Stores .....	G-1
Appendix H	FEMA IT Architectural Principles and Supporting Rationale .....	H-1
Appendix I	Executive Directives, Congressional Acts, and Judicial Guidance Affecting the <i>FEMA IT Architecture</i> .....	I-1
Appendix J	Operational Environmental Factors Influencing FEMA IT Systems .....	J-1
Appendix K	Cross-Cutting Issues Associated with Development of the Technical Reference Model and Standards Profile .....	K-1
Appendix L	Major IT Needs and Requirements of FEMA Organizational Elements.....	L-1
Appendix M	Catalog of FEMA Enterprise-Wide Systems.....	M-1
Appendix N	Identification and Description of Major FEMA IT Services in the Technical Reference Model (TRM) .....	N-1
Appendix O	Profiles of Major IT Standards .....	O-1



## Foreword

This document is the Federal Emergency Management Agency's (FEMA's) initial *Information Technology (IT) Architecture* prepared under the *Information Technology Management Reform Act (ITMRA)* with the supporting guidance of OMB Memorandum M-97-16.

The document is written to be primarily directive in nature to identify and define common high-level IT architectural standards and components that can be reused across FEMA systems.

**Assumptions and Constraints.** The following are the basic assumptions and constraints:

- **Unclassified operations only.** To make this document accessible to the widest possible audience, the initial *IT Architecture* was developed and defined for unclassified operations only. It is anticipated that future revisions to the *FEMA IT Architecture* will have a classified annex. In related activity, FEMA is in the process of developing plans, policies, and security architecture components in response to the Critical Infrastructure Protection (CIP) program under Presidential Decision Directive 63 (PDD-63).
- **Status of business function allocation.** In developing the *FEMA IT Architecture*, over 500 highly detailed FEMA business functions for FEMA's Directorates and Administrations, Divisions, and Branches currently documented in FEMA's *Missions and Functions Manual* were reviewed and considered. Nearly all of the business functions were determined to be information technology significant to some degree.
- **Need to Conduct Business Case Analysis.** An important constraint to note is that some of the architectural components and technology may not make sound business sense given the current state of FEMA networks. For example, advanced groupware technologies such as intelligent collaboration and visualization of very large GIS data sets; integrated voice, video, and data applications; distributed interactive simulation (DIS); and distance learning (incorporating virtual reality technology) are widely accepted to be bandwidth intensive in large-scale distributed operations. The current FEMA network has limited capability to support some of these advanced technologies. Accordingly, it is important to realize that this *FEMA IT Architecture* merely provides an architectural framework for discussing how FEMA IT systems might be structured to use common architectural components that are of potential interest across a number of FEMA business units. Business case analyses for some of the more demanding architectural components clearly need to be accomplished before any actual implementation.
- **A Snapshot in time.** It was assumed that business process re-engineering (BPR) was beyond the scope of this initial *FEMA IT Architecture*. Within FEMA, improvement efforts and re-organization are in process. The *FEMA IT Architecture* will be updated as reorganizations of various parts of the Agency occur or as business processes in the Agency are re-engineered. This *FEMA IT Architecture* will encourage the enterprise-wide adoption of common architectural components, wherever possible. It sets the stage for development of an integrated IT investment strategy with detailed cost-benefit analyses for selected procurements.
- **Large requirement for enterprise information flow and many program-centric systems.** Another important consideration in the development of this initial *FEMA IT Architecture* is that over 100 FEMA organizational entities have business associations

with well over 200 other external agencies, activities, and partners. Most of these interactions were also determined to be IT significant. Further complicating the analysis was the identification of a comparatively large number of standalone program-centric legacy systems and document and data stores within the various FEMA groups. These legacy systems and document/data stores present challenges for future enterprise-wide IT integration. The analysis clearly pointed to the need for universally accepted standards to achieve information exchange and interoperability among heterogeneous systems.

With the large number of IT-significant business functions, the large number of associated IT systems and data stores, and the large number of internal and external collaborating organizations, this initial *IT Architecture* document addresses the business functions at a high-level. For each business function, FEMA can provide additional supporting details, if required. FEMA has started development of an *IT Architecture* Data Base to identify and address architecture components for all of the business functions. Future revisions to this document and the development of the ancillary electronic *IT Architecture* Data Base (described in Section 1.12.1) should help address business functions, information flows, systems/applications, and data stores at progressively finer levels of detail in future revisions to this document.

**Use of Terminology.** Within the context of the directive tone noted above, the following terms have these meanings:

- The use of the term ***shall*** implies that the statement is mandatory for compliance in the development of future IT systems or for systems that are proposed to be re-engineered. Requests for waivers must be justified and require formal action by the FEMA Information Resources Board (IRB) in accordance with the provisions contained in Section 4 of this document.
- The use of the term ***will*** implies an intent to consider the requirement in earnest in the development of future IT systems or systems that are proposed to be re-engineered. In general, *IT Architecture* requirements characterized as *will* can be expected to have viable alternatives. In the interest of architectural standardization, proposed systems that do not comply with a *will* requirement must also request a waiver, but the burden-of-proof will not be as stringent.
- The use of the terms ***must, is declared to be, or is determined to be*** should be interpreted in the same sense as the term *shall*.
- The use of the terms ***may, might, could, should*** is intended to be only advisory in nature. At some point in the future, the architectural requirement may be tightened to *will* or *shall* status. There is no requirement to request a waiver or deviation from these standards from the IRB for future IT systems or those proposed to be re-engineered. However, the waiver must be noted in the systems development documentation and must be addressed as appropriate in systems engineering reviews.

Within the Technical Reference Model (Section 2), the following terms have the meaning as indicated:

- ***Adopted*** means that the standard or standard tool has been formally accepted by the CIO for the service area or architectural component to which it refers.

- ***Under evaluation*** means that the standard or standard tool has not yet been formally accepted and is being actively evaluated or considered within FEMA.
- ***Suggested*** is a less strong term than *under evaluation*. *Suggested* really means that there is a potential opportunity for technology insertion or standardization that ought to be more formally considered – business case and funding permitting.
- ***In-service use*** means that the standard or tool is currently being used within FEMA IT systems. It is subject to re-evaluation, re-engineering, or additional development prior to being formally adopted.

**Mandatory Compliance Statement.** This *FEMA IT Architecture* is mandatory for compliance on the development of new IT systems and any proposed re-engineering, re-hosting, or additional development of legacy systems. Section 4 provides amplifying information.

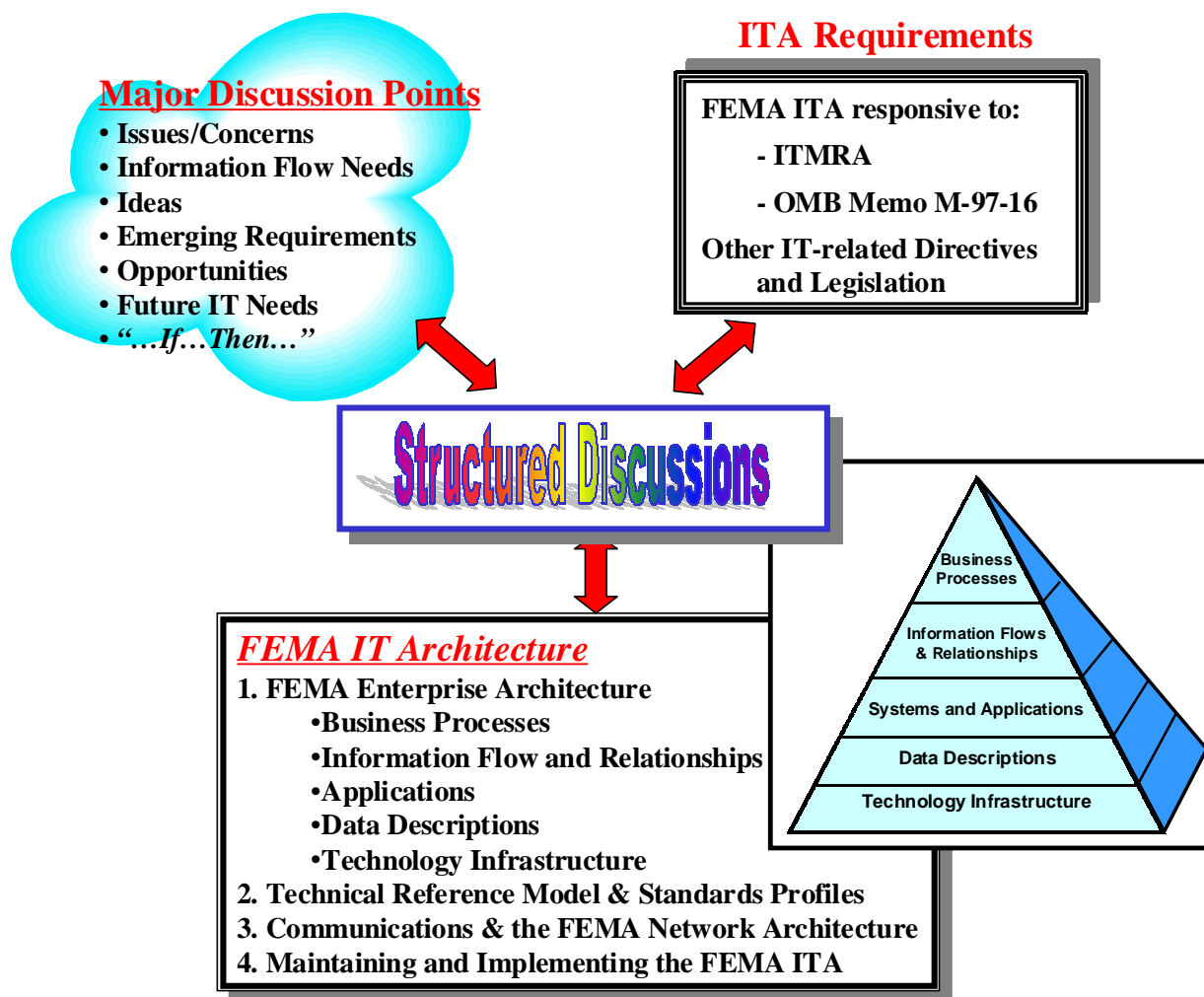
**Point of Contact.** The point of contact for questions or comments regarding this *FEMA IT Architecture* is G. Clay Hollister, FEMA Chief Information Officer (CIO), at (202) 646-3006. His e-mail address is Clay.Hollister@fema.gov.

This page intentionally left blank

## Executive Summary

**Introduction.** The Federal Emergency Management Agency (FEMA) is the Federal governmental unit that bears primary responsibilities for the nation's emergency management system. When devastation is serious and exceeds the capability and resources of local and State governments to respond, States turn to the Federal government for help and assistance. Once the President has declared a major disaster or emergency, FEMA coordinates not only its own response activities but also those of as many as 27 other Federal agencies.

**Methodology and Approach.** This document is FEMA's initial *IT Architecture*. As illustrated below, the *Architecture* was developed through a series of structured discussions across FEMA Headquarters and Regional staff. The structured discussions mirrored the architectural *pyramid* implied by OMB Memorandum M-97-16. This *IT Architecture* document closely follows that approach.



As the length of the discussions permitted, the following architectural components were addressed:

- Business functions
- Subactivities

- **Inputs and outputs**
- **Operational environmental factors**
- **Systems and applications**
- **Documents and data stores**
- **Technologies and security components.**

The results of these discussions led to the development of the target *FEMA IT Architecture* with the following major characteristics:

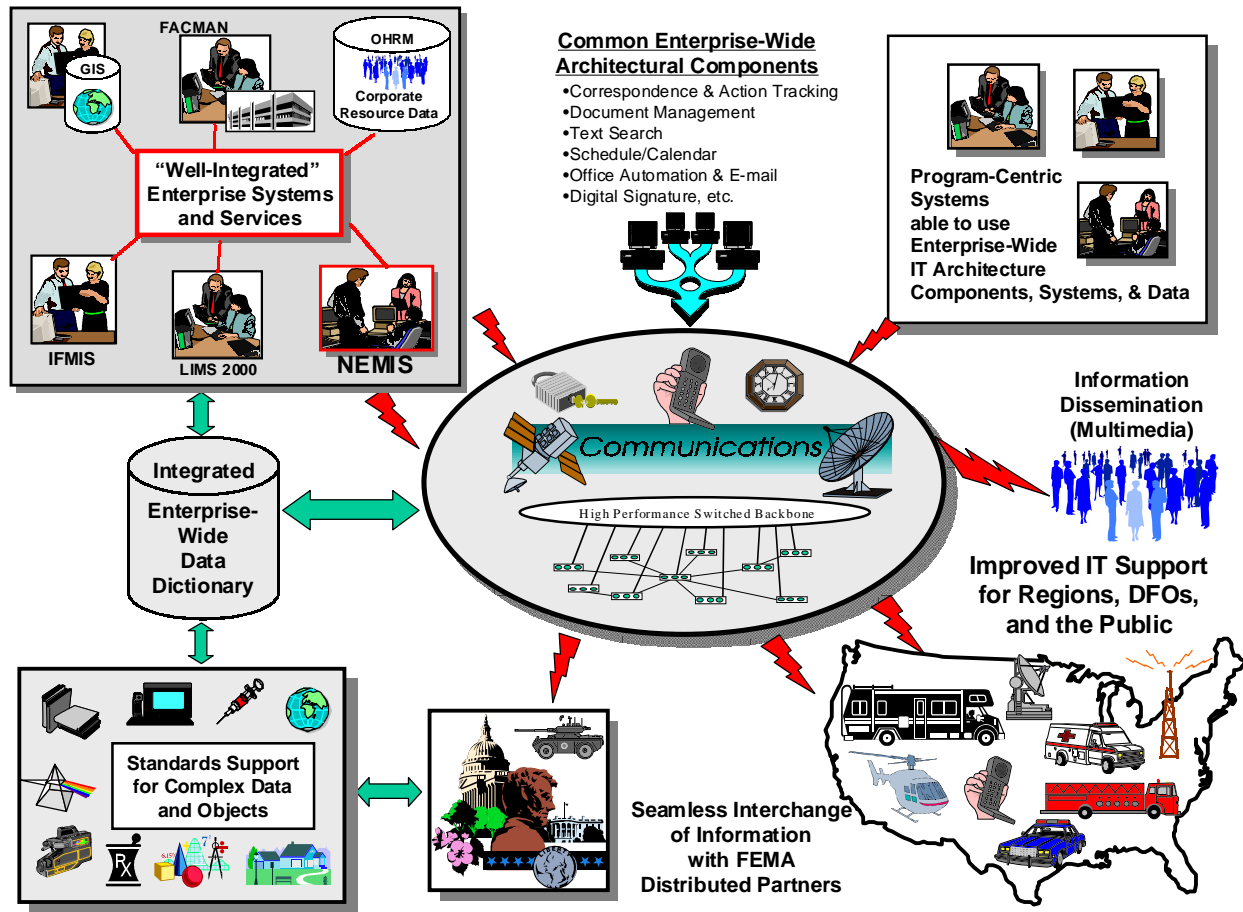
- **Well-integrated enterprise-wide systems and services**
- **Improved communications and networking**
- **Consideration of impact on legacy telecommunications systems as new capability is added**
- **Adequate bandwidth for advanced IT applications**
- **Potential for increased connectivity**
- **Achieving a consensus on standards across the enterprise**
- **Engineering concerns addressed**
- **Emphasis on open systems standards**
- **Improved data integrity over the life cycle.**

Because of FEMA's significant investment in the National Emergency Management Information System (NEMIS), this target *FEMA IT Architecture* has designated NEMIS as an IT architectural *cornerstone*. Within FEMA, NEMIS is the lead system for providing comprehensive mission support, interoperability, and re-use. NEMIS is a proving ground for implementing advanced IT concepts. While NEMIS is an architectural *cornerstone*, the *FEMA IT Architecture* is open to good ideas and innovation from any enterprise-wide system. This *FEMA IT Architecture* considers such IT concepts as:

- Developing integrated enterprise-wide systems and services and a common data dictionary.
- Developing common and re-usable enterprise-wide IT architectural components based on open systems approaches that can be used by both enterprise-wide and program-centric systems.
- Developing, re-engineering, consolidating, and re-hosting selected program-centric systems to be compliant with the architecture and the enterprise-wide data dictionary.
- Providing an enterprise approach for systems engineering and configuration management.
- Enhancing the FEMA communications backbone to provide improved IT support and improved Quality of Service to the Regions, Disaster Field Offices (DFOs), and the public.
- Exploring the potential for improved connectivity with FEMA's business partners, Regions, States, and local government through establishment of Extranets and Virtual Private Networks (VPNs).
- Achieving consensus on approaches for creating, managing, using, and interchanging complex documents and data sets in an intelligent manner across the enterprise.
- Performing technology insertion in such areas as digital libraries, distributed collaboration tools, distance learning, interactive GIS, secure electronic commerce, virtual reality, simulation, and other emerging technologies as added IT support to FEMA business processes.

As a matter of high priority and in response to Presidential Decision Directive 63 (PDD-63), the FEMA CIO, in the role of FEMA's Chief Information Assurance Officer (CIAO), is currently in the process of developing a comprehensive plan for protecting FEMA's critical IT systems and networks. This *IT Architecture* is consistent with that direction and firmly establishes and validates many of the underlying operational requirements of the Critical Information Protection (CIP) program.

**FEMA Information Systems Landscape.** The target *FEMA IT Architecture* is depicted in the following graphic.



This page intentionally left blank